UNITED STATES OF AMERICA	)	
	)	**Prosecution Supplement**
v.	)	
	)	**to Prosecution Proposed**
Manning, Bradley E.	)	**Case Calendar**
PFC, U.S. Army,	)	
HHC, U.S. Army Garrison,	)	
Joint Base Myer-Henderson Hall	)	**8 March 2012**
Fort Myer, Virginia 22211	)	

The United States respectfully requests the Court deny Defense Proposed Case Management Order (hereinafter "Defense's Proposal") and instead adopt the Prosecution Proposed Case Calendar Update (hereinafter "Prosecution's Proposal") for the reasons that follow.

I: ADMINISTRATIVE CASE BACKGROUND.

1. The accused is charged with Aiding the Enemy by Giving Intelligence, a violation of Article 104, UCMJ. The accused is also charged under Article 134, UCMJ, with transmitting national defense and foreign relations information to persons or organizations not entitled to receive it, in violation of 18 U.S.C. § 793(e) and 18 U.S.C. § 1030(a)(1). Finally, the accused is charged under Article 134 with stealing government property, in violation of 18 U.S.C. § 641, and various offenses under Article 92, UCMJ.

2. This case involves both classified and unclassified information in significant volume. Additionally, the government's charges involve completed offenses, not attempts. As a result of the substance of the charged compromises of classified and unclassified information, the United States Government's response has been widespread, spanning multiple Executive Branch departments, agencies, and military commands (hereinafter "federal organizations"), and requiring interagency coordination in response to the national security issues raised by the compromises.

II: CLASSIFIED INFORMATION.

1. Information may be originally classified only if done so by an original classification authority (OCA). Executive Order 13526 § 1.1(a). Additionally, the information must be owned by, produced by or for, or under the control of the United States Government and must fall within one or more of the following categories: military plans, weapons systems, or operations; foreign government information; intelligence activities (including covert action), intelligence sources or methods, or cryptology; foreign relations or foreign activities of the United States, including confidential sources; scientific, technological, or economic matters relating to the national security; United States Government programs for safeguarding nuclear materials or facilities; vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security; or the development, production, or use of weapons of mass destruction. See Executive Order 13526 §§ 1.1(a), 1.4(a)-(h). Finally, the OCA must determine "that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security" and be able to identify or describe the

expected damage. See Executive Order 13526 § 1.1(a) (emphasis added). OCAs make their classification designations based on their authority under Executive Order 13526, Classified National Security Information (signed by President Barack Obama on 29 December 2009) or for materials classified prior to 27 June 2010 on Executive Order 12958 (signed by President Clinton on 17 April 1995 and amended by Executive Order 13292 signed by President Bush on 25 March 2003), as well as relevant classification guides.

2. The authority to classify information is limited to (1) the President and the Vice President; (2) agency heads and officials designated by the President; and (3) United States Government officials delegated this authority pursuant to paragraph (c) of section 1.3(a). Executive Order 13526 § 1.3(a).

III: ACCESS TO CLASSIFIED INFORMATION BY THE ACCUSED AND DEFENSE COUNSEL.

1. Attorneys representing military personnel are considered persons outside the Executive Branch, regardless of any military affiliation the attorney may have. See Executive Order 13526; Army Regulation 380-67, Personnel Security Program, 9 September 2008 with Rapid Action Review, 4 August 2011, paragraph 3-23f (hereinafter "AR 380-67"). As such, disclosure of classified information to defense counsel is governed by the rules for disclosing classified information to any individuals or agencies outside of the Executive Branch. Therefore, in a military justice case involving classified information, the trial counsel is prohibited from providing defense counsel with copies of, or access to, classified information, unless preapproved by the appropriate authority. Id. The Deputy Chief of Staff for Intelligence, United States Army, or his delegate, is the approving authority for granting security clearances and general access to classified information within the Army and for courts-martial. Id. However, before disclosing any classified information to defense counsel, the trial counsel must have authority from the OCA of the federal organization that "owns" the classified information. See Executive Order 13526. In this case, the accused, all defense counsel, and all expert consultants appointed to the defense team have been granted security clearances and general access to classified information.

2. Authority to disclose classified information to the accused and defense counsel generally begins with a request from the trial counsel to a federal organization's litigation division or general counsel's office. See Enclosure 1 (Sample Request for Consent to Disclose Classified Information to the Accused and the Defense, dated 14 March 2011). The assigned attorney from the organization usually works with experts to attempt to identify the specific OCA from within the organization for the requested classified information. Many federal organizations have many OCAs, with each OCA responsible for different categories of classified information within the federal organization. After the litigation attorney identifies the component/department or OCA responsible for the information and makes a recommendation as to disposition, the information is typically reviewed for classification to determine if the underlying information is too sensitive to turn over to the defense. This decision is made by balancing the ongoing national security concerns with granting access to the accused and defense counsel, as well as determinations concerning whether an alternative is adequate.

3. Once the OCA who owns the actual document approves the request and authorizes disclosure of the information, the document is vetted to ensure there are no other OCAs within the executive branch that have classified information equities within the document. In many cases, intelligence work-product contains sources from across the intelligence community, particularly analytic reports or assessments. In the case of a classified analytic report or assessment, the product could involve the equities of several OCAs, requiring the classified information to be vetted through other federal organizations with interests, before disclosure to the defense. Many of the classified documents in this case contain classified information owned by several different OCAs. In this case, the accused, all defense counsel, and all expert consultants have been granted access to the classified documents, which make up the bases for many of the charges and their specifications.

IV: CATEGORIES OF CLASSIFIED INFORMATION INVOLVED IN THIS CASE.

The classified information in this case can be characterized in three different categories: (1) the charged documents or information, which serve as the basis for many of the charges and their specifications; (2) other classified evidence, produced by the United States, applicable to the case-in-chief; and (3) other classified evidence.

1. The charged documents or information, which serve as the basis for many of the charges and their specifications.

When the United States refers to classified "charged documents or information" relating to this case, including databases containing classified information, it is referring to the datasets listed below, as described in the relevant classification reviews.

A. Combined Information Data Network Exchange Iraq (CIDNE-I). CIDNE-I is a Department of Defense database containing more than 300,000 Significant Activity (SIGACT) reports regarding the Iraq war, many of which included information pertaining to military plans, weapons systems, operations, and improvised explosive device attacks. See CENTCOM Classification Review, 21 October 2011, BATES 00376893 (enclosed in Enclosure 1 to Supplement to Prosecution Motion for Protective Order, dated 8 March 2012).

B. Combined Information Data Network Exchange Afghanistan (CIDNE-A). CIDNE-A is a Department of Defense database containing more than 91,000 SIGACT reports regarding the Afghanistan war, many of which included information pertaining to military plans, weapons systems, operations, and improvised explosive device attacks. See CENTCOM Classification Review, 21 October 2011, BATES 00376889 (enclosed in Enclosure 1 to Supplement to Prosecution Motion for Protective Order, dated 8 March 2012).

C. Two analytic products produced by a government intelligence agency containing classified information. See Classification Review, 31 October 2011, BATES 00378151 (enclosed in Enclosure 1 to Supplement to Prosecution Motion for Protective Order, dated 8 March 2012).

D. Multiple classified documents from an Army Regulation 15-6 investigation relating to a military operation in Farah Province, Afghanistan in May 2009. Many of these documents included information pertaining to military plans, weapons systems, operations, vulnerabilities or capabilities of systems, and code words identified with mission operations. See CENTCOM Classification Review, 21 October 2011, BATES 00376902 (enclosed in Enclosure 1 to Supplement to Prosecution Motion for Protective Order, dated 8 March 2012).

E. A video from an Army Regulation 15-6 investigation relating to a military operation in Farah Province, Afghanistan in May 2009. See CENTCOM Classification Review, 21 October 2011, BATES 00376902 (enclosed in Enclosure 1 to Supplement to Prosecution Motion for Protective Order, dated 8 March 2012).

F. An analytic product produced by an Army intelligence organization containing classified information. See Classification Review, 2 December 2012, BATES 00410626 (enclosed in Enclosure 1 to Supplement to Prosecution Motion for Protective Order, dated 8 March 2012).

G. Net-Centric Diplomacy (NCD) and Department of State Cables. NCD is a Department of State database containing more than 280,000 diplomatic cables or messages concerning foreign relations or foreign activities of the United States. See Department of State Classification Review, 30 October 2011, BATES 00376904-5 (enclosed in Enclosure 1 to Supplement to Prosecution Motion for Protective Order, dated 8 March 2012).

H. A United States Southern Command (SOUTHCOM) database. This database contains more than 700 records, many of which contain intelligence sources and methods. See SOUTHCOM Classification Review, 4 November 2011, BATES 00378647 (enclosed in Enclosure 1 to Supplement to Prosecution Motion for Protective Order, dated 8 March 2012).

2. Other classified evidence, produced by the United States, applicable to the case-in-chief.

In addition to the charged documents, the United States intends to use classified information as evidence to prove the elements of many of the specifications. As part of the discovery process, the United States produced other pieces of classified information after coordination with, and the approval of, the different OCAs. This information generally falls within two sub-categories: (A) digital media, including associated forensic reports and data extracted from the media, and (B) audit data or "logs" collected from SIPRNET systems.

A. Digital media, including associated forensic reports and data extracted from the media.

(1) The United States Army Criminal Investigative Command (CID) collected more than fifty individual digital media devices. After initial forensic examination, CID determined that twenty-three contained relevant information pertaining to the accused, and completed a full forensic examination of these hard drive and removable media drives. At least twenty of these devices contained classified information, and many contained the analytic work

product of intelligence analysts. Specifically, the work computers used by the accsued contained classified information owned by multiple federal organizations and OCAs.

(2) Prior to producing forensic images of the collected drives, and the derivatively classified forensic reports, trial counsel had to consult with each federal organization and their OCAs that had an equity in the drives. After conducting a due diligence search of the drives with the assistance of security experts, trial counsel sent requests for consent to produce classified information in discovery to the OCAs of the charged documents or information, and any other OCAs that could reasonably be identified during the search of the hard drives. Based on classified information being inextricably commingled on the digital media, trial counsel was required to withhold discovery until consent was received from all the relevant OCAs, either because they were the OCA of a charged document or because they were an OCA identified as a result of the due diligence search of the digital media. See Enclosure 1 (Sample Request for Consent to Disclose Classified Information to the Accused and the Defense, dated 14 March 2011). The Government will have to employ a similar "due diligence" process to identify OCAs for any other classified digital media ordered to be produced in this case.

B. Audit data collected from SIPRNET systems. Based on the charged misconduct originating from the use of SIPRNET computers in Iraq, CID collected multiple sets of audit data (hereinafter "logs") for computer networks, databases, and systems. These logs were collected from five federal organizations. Many of the logs are completely classified, while others contain unclassified and classified information. Additionally, some of the logs contain search terms used on SIPRNET, which may also be classified. See Enclosure of Enclosure 1 to Supplement to Prosecution Motion for Protective Order, dated 8 March 2012.

3. Other classified evidence or information.

A. The prosecution intends to present or otherwise produce additional classified information as part of its presentencing case. Additionally, mitigation evidence may exist, which the prosecution recognizes it must produce in some form. Furthermore, the Court may compel the production of other information, such as a classified assessment, as a result of the defense motion to compel discovery. At this time, the prosecution believes that the Court's order to produce any assessment, if one exists, would likely require the coordination of a minimum of three federal organizations and their OCAs.

B. For example, the Secretary of Defense directed the Defense Intelligence Agency (DIA) to establish the Information Review Task Force (IRTF) to lead a comprehensive Department of Defense review of classified documents posted to the WikiLeaks website—a review of everything released, including Department of State (DoS) information, from the DoD perspective. See Enclosure 2 (Secretary of Defense, Memorandum, dated 5 August 2010). As a result, if the Court compels the production of the IRTF report, that report will, at the very least, require coordination with the Department of State before a decision may be made on classification, disclosure, or asserting the MRE 505 privilege.

C. In preparation for litigation, trial counsel have also actively sought to review certain information from multiple federal organization. See Enclosure 3 (Sample Search and

Preservation Request, dated 14 June 2011). After reviewing tens-of-thousands of pages of documents from multiple federal organizations pursuant to these requests, trial counsel are confident that other analytic products produced within the intelligence community contain references to information otherwise "owned" by other organizations within the intelligence community; therefore, any production of this material will likely take time to coordinate because of all the parties involved.

V: ORIGINAL CLASSIFICATION AUTHORITIES

1. As discussed above, the case involves multiple federal organizations because of the scale of the alleged disclosures of classified information. These organizations fall within the three categories below. If a federal organization contains an "*" next to its name, the United States anticipates that documents originating from that federal organization will contain information from multiple OCAs.

A. Federal organizations with equities in charged documents or digital forensic evidence.

(1) Department of State*
(2) Office of the Director of National Intelligence
(3) Defense Information Systems Agency
(4) United States Central Command
(5) United States Southern Command
(6) Government Agency*
(7) United States Cyber Command

B. Other federal organizations with equities, but not in charged document or digital forensic evidence.

(1) Federal Bureau of Investigation
(2) Government Agency*
(3) Department of Defense*
(4) Defense Intelligence Agency*

C. Other federal organizations that have very limited involvement

2. The United States estimates that any Court order to disclose classified information, will likely require coordination with multiple federal organizations in categories (1) and (2), and roughly estimates **forty-five to sixty days** to aggressively coordinate a response across all equity holders. Within the sixty day window, it would likely take approximately one to two weeks to identify equity holders and distribute the product amongst the relevant federal organizations and their OCAs. Thirty days to analyze the product to identify the sources of classified information and evaluate the level of protection that must be given to that information. Two additional weeks for the OCAs to coordinate a response, for example to approve full disclosure, limited disclosure, some variation, or invoke the privilege. If an OCA invokes the classified information privilege, it may take additional time to conduct a classification review and route the document to the

"head of the executive or military department or government agency concerned" for proper invocation. See MRE 505(c).

VI: USE OF CLASSIFIED INFORMATION DURING TRIAL

1. Issues relating to classified information are likely to arise in connection with the use of such information during trial. Under MRE 505(h), if the accused reasonably expects to disclose or cause the disclosure of classified information in any manner in connection with a court-martial proceeding, the accused must provide notice to the United States to allow the United States the opportunity to be heard utilizing the procedures outlined under MRE 505(i). In this case, the United States does not anticipate extensive litigation during this phase. However, depending on what information the accused intends to disclose or cause the disclosure of at trial, the process could be somewhat lengthy if the United States needs to contact an OCA or multiple OCAs for a classification review of the material.

2. With respect to the use of classified information by the United States during trial, the United States expects to use classified information during the merits and presentencing phases of the court-martial. Assuming the Court sets a date closer to trial to consider whether the standard for closure of the courtroom is met under RCM 806(b)(2), the United States expects to have an evidence presentation plan in place for the court's consideration that is narrowly-tailored to protect classified information and the accused's right to, and the public's interest in, a public trial. Additionally, the United States intends to file a motion *in limine* seeking a preliminary ruling on the admissibility of certain classified evidence in an attempt to minimize issues at trial. Because the substance of the classified information will likely be relevant to a determination of whether the evidence is admissible, the United States expects to file a motion requesting the Court close the courtroom during this proceeding as well. Finally, the defense may also file a motion *in limine* seeking a preliminary ruling on the admissibility of classified evidence, if the defense contends that certain classified evidence is more prejudicial than probative.

VII: CONCLUSION

Classified information litigation is a complex area of law. In the case at bar, the complexity is magnified given the amount of information allegedly compromised. In light of the above issues, the United States respectfully requests the Court adopt the Prosecution's Proposal.

ASHDEN FEIN
CPT, JA
Trial Counsel

I certify that I served or caused to be served a true copy of the above on Defense Counsel, via electronic mail, on 8 March 2012.

ASHDEN FEIN
CPT, JA
Trial Counsel